Kirka Lintula

VIRTUAALITYÖPÖYDÄN KÄYTTÄMINEN MOBIILILAITTEELLA

Tietojenkäsittelyn koulutusohjelma

2014

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

VIRTUAALITYÖPÖYDÄN KÄYTTÄMINEN MOBIILILAITTEELLA

Lintula, Kirka
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Toukokuu 2014
Ohjaaja: Grönholm, Jukka
Sivumäärä: 32
Liitteitä: 0

Asiasanat: virtualisointi, mobiililaite, BYOD

Opinnäytetyön aiheena oli tutkia omien kannettavien laitteiden käyttöä työpaikalla sekä mobiilivirtualisoinnin mahdollisuuksia ja toteutustapoja. Tavoitteena oli tutustua eri valmistajien tarjoamiin ja tuottamiin palveluihin, sekä siihen miten näitä voitaisiin käyttää hyödyksi erityyppisissä tilanteissa.

Tutkiessani aihetta, tuli selväksi se, että palveluntarjoajat ja sovelluskehittäjät haluavat kehittää entistä helpommin lähestyttäviä sekä monilla alustoilla pyöriviä järjestelmiä. Tämä asettaa ohjelmistonkehitykselle luonnollisesti haasteita, mutta tuo loppukäyttäjälle helppoutta.

Omien laitteiden käyttö työpaikalla on alati kasvava trendi, joka monessa tapauksessa helpottaa työtä, mutta tuottaa myös hankaluuksia tietoturvan suhteen. Yritysten tuleekin pitää huoli siitä, että arkaluontoinen data saadaan pidettyä omissa käsissä turvattuna.

VIRTUAL DESKTOP USAGE WITH MOBILE DEVICE

Lintula, Kirka
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in information technology
May 2014
Supervisor: Grönholm, Jukka
Number of pages:32
Appendices:0

Keywords: virtualization, mobile device, BYOD

The purpose of this thesis was to research the usage of ones own mobile device at work and mobile virtualizations possibilities and different ways to produce them. The aim was to get to know different manuafacturers services and implementation processes, and also how they can be used for the benefit of different situations.

While studying the topic, it became clear that service providers and application developers want to develop a more easily approachable systems that also run in many different platforms. This poses challenges for the software development of course, but increases the end-user convenience.

Using your own devices at workplace is an ever growing trend, which in many cases eases the work itself, but causes difficulties considering the IT-security. The companies must be sure, that the data is being kept secured in their own hands.

SISÄLLYS

1 JOHDANTO

Tämän työn tavoitteena oli tutkia ja selvittää virtuuualityöpöydän käyttöä mobiililaitteilla. Käyn työssäni läpi virtualisointia ja sen teoriaa yleisesti, jonka kautta pyrin selvittämään virtualisoinnin tuomia mahdollisuuksia eri mobiilipäätteillä ja muilla kannettavilla laitteilla sekä toteutustapoja ja eri ohjelmistovalmistajien tarjoamia ratkaisuja.

Työssä on pyritty ottamaan huomioon erityisesti virtualisoinnin kautta saavutetut hyödyt ja haitat yritysten toimintaan sekä itse työntekoon. BYOD- mallin (Bring Your Own Device) yhä nouseva kiinnostus yrityksissä ja työntekijöissä asettaa yritykset haastavaan tilanteeseen tietoturvan, laitteistohankintojen sekä ylläpidon osalta. Koska kyseinen teknologia on vasta tulossa enenevissä määrin yrityksissä käyttöön, tuleekin punnita tarkasti hyödyt ja haitat, että kannattaako mobiilivirtualisointia lähteä toteuttamaan.

Omien laitteiden käyttö yritysmaailmassa on jo nyt tätä päivää ja teknologian kehittyessä onkin myös yritysten muutettava omia toimintatapojaan, jotta liiketoiminnasta saadaan mahdollisimman tehokasta, ottaen huomioon myös työntekijät ja heidän toiveensa.

Mobiililaitteitteiden yleistymisen johdosta tulee tietoturvaan kiinnittää erityistä huomiota. Kannettavien tietokoneiden, tablet-laitteiden ja kännyköiden toimiessa eri käyttöjärjestelmillä sekä yrityksen sisällä, että sen ulkopuolella, tulee tietoturvastrategiaa hioa käytettävyyden ja sujuvuuden ehdoilla. On myös tärkeää pystyä erottelemaan henkilökohtaiset ja yrityksen omat sovellukset, jotta tietoturvariskit saadaan minimoitua. Yritykset pyrkivätkin pitämään lankoja omissa käsissään ainakin datan osalta, jonka halutaan säilyvän yrityksen omassa verkossa ja näinollen paremmin suojattuna. Datan liikkuvuudesta pitää myös huolehtia niin, ettei arkaluontoinen materiaali päädy ulkopuolisiin sovelluksiin tai vääriin käsiin. Kannettavilla laitteilla tämä on erityisen tärkeää, sillä pienet laitteet hukkuvat helposti tai saattavat tulla varastetuiksi.

Toimistotyötä tehdään nykyään monesti työpaikan ulkopuolellakin ja mobiilipäätteillä työskentely edellyttää toimivaa ratkaisua etätyöskentelyn mahdollistamiseen. Alan johtavissa ohjelmistoratkaisuissa etätyöskentely onkin otettu huomioon kiitettävällä tasolla ja monesti käyttäjällä on mahdollisuus muodostaa suojattu yhteys yrityksen verkkoon ja järjestelmiin käyttäen eri tekniikoita.

2 VIRTUALISOINTI YLEISESTI

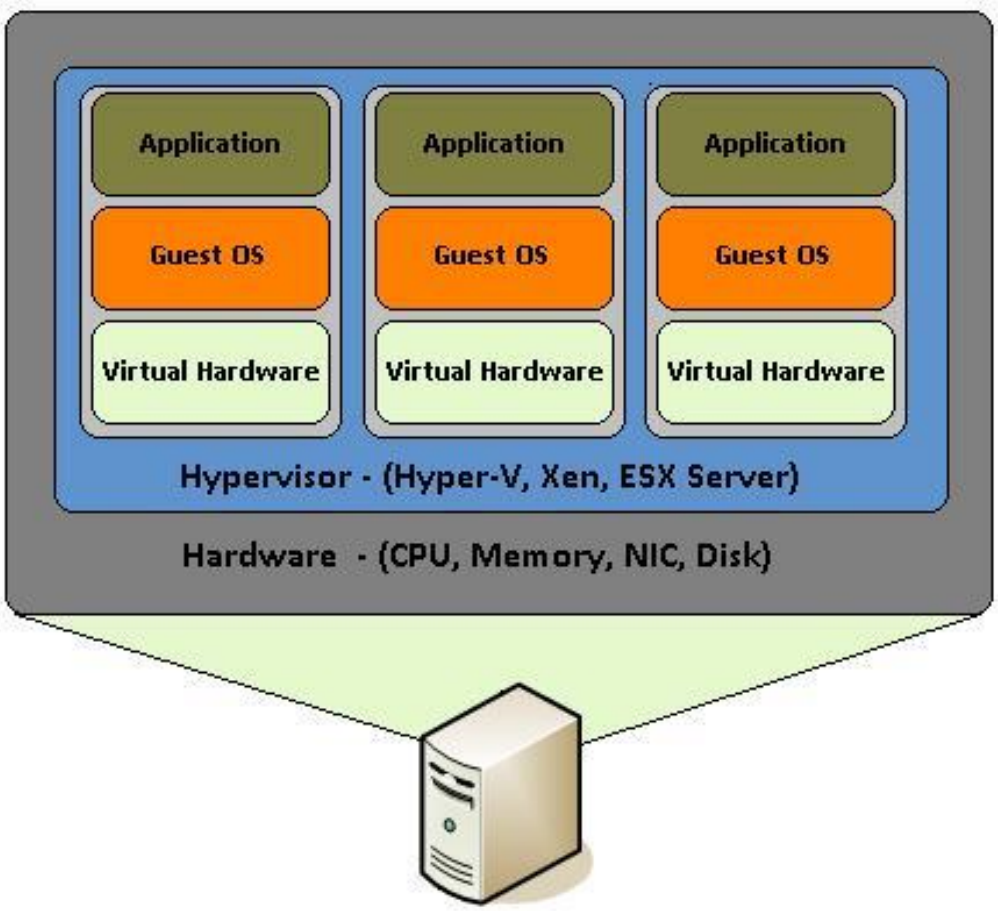
2.1 Virtualisoinnin historia

Virtualisoinnin juuret juontavat 1960-luvulle, jolloin Professori Christopher Strachey tutustutti ihmisille termin osituskäyttö (time-sharing) teoksessaan Time Sharing in Large Fast Computers. Kyseessä oli tapa ohjelmoida siten, että samalla kun Strachey kirjoitti koodia, toinen ohjelmoija pystyi samaan aikaan tekemään virheenkorjausta. Strachey kutsui tätä tapaa moniajo-ohjelmoinniksi (multi-programming). (Dittner & Rule 2007.). Myös IBM oli kiinnostunut virtualisoinnista 1960-luvulla. Se kehitti suurtietokoneiden aikakaudella virtualisointiin perustuvaa keskuskonetta CP-40. Se ei kuitenkaan koskaan tullut myyntiin asiakkaille ja järjestelmä jäi ainoastaan laboratoriokäyttöön, mutta kyseisestä käyttöjärjestelmästä jatkokehitettiin uusi, kaupallinen, keskuskone CP-67, jossa käytettiin käyttöjärjestelmää CP/CMS. CP/CMS- lyhenne tulee sanoista Control Program ja Console Monitor System. CMS oli vuorovaikutteinen yhden käyttäjän käyttöjärjestelmä. CP:n tehtävänä oli toimia keskuskoneessa luoden virtuaalikoneita. Virtuaalikoneet taas ajoivat CMS-käyttöjärjestelmän, jonka kanssa käyttäjä pääsi toimimaan. (Conroy, 2010.)

Virtuaalikoneiden avulla pystyttiin jakamaan keskuskoneen resursseja, eikä näitä keskuskoneen resursseja ollut pakko jakaa tasan kaikkien käyttäjien kesken. Näin ollen resursseja pystyttiin jakamaan käyttäjien tarpeiden mukaan. Kyseessä oli myös turvallisuustekijä, sillä nyt yksi käyttäjä ei pystynyt kaatamaan koko keskuskonetta, vaan ainoastaan oman virtuaalikoneensa. (Conroy, 2010.)

Virtualisoinnin kehitys jatkui edelleen ja 1980-luvulla uudet yritykset, kuten AT&T, Microsoft ja Locus Computing Company, kehittivät sovellusvirtualisointia sekä virtuaaliverkkoja. Myöhemmin 1990-luvulla Apple kehitti Macintosh-koneelleen virtuaaliseen ajoon pystyvän Connectix Virtual PC:n, jolla pystyttiin ajamaan Microsoft Windowsia Macintoshilla. VMware nousi virtualisointikartalle vuonna 1998. Siitä tuli nopeasti teknologian kärkikehittäjä ja se toikin ensimmäisenä markkinoille täysvirtualisointiin pystyvän tuotteen. (Wikimedia Foundation, 2010.)

Vuosituhannen vaihteen jälkeen alettiin tuoda avoimeen lähdekoodiin perustuvia, ilmaisia virtualisointisovelluksia. XenSource, Inc- yhtiön Xen-virtualisointisovelluksesta tuli maailman ensimmäinen avoimen lähdekoodin virtualisointisovellus vuonna 2003. Myös VMware alkoi tarjoamaan ilmaisia virtualisointisovelluksiaan, VMware Player sekä VMware Server, vuosina 2005 ja 2006. (Wikimedia Foundation, 2010.)



KUVA 1. Laitteistovirtualisointi. (wikimedia, 2010)

2.2 Työasemavirtualisointi

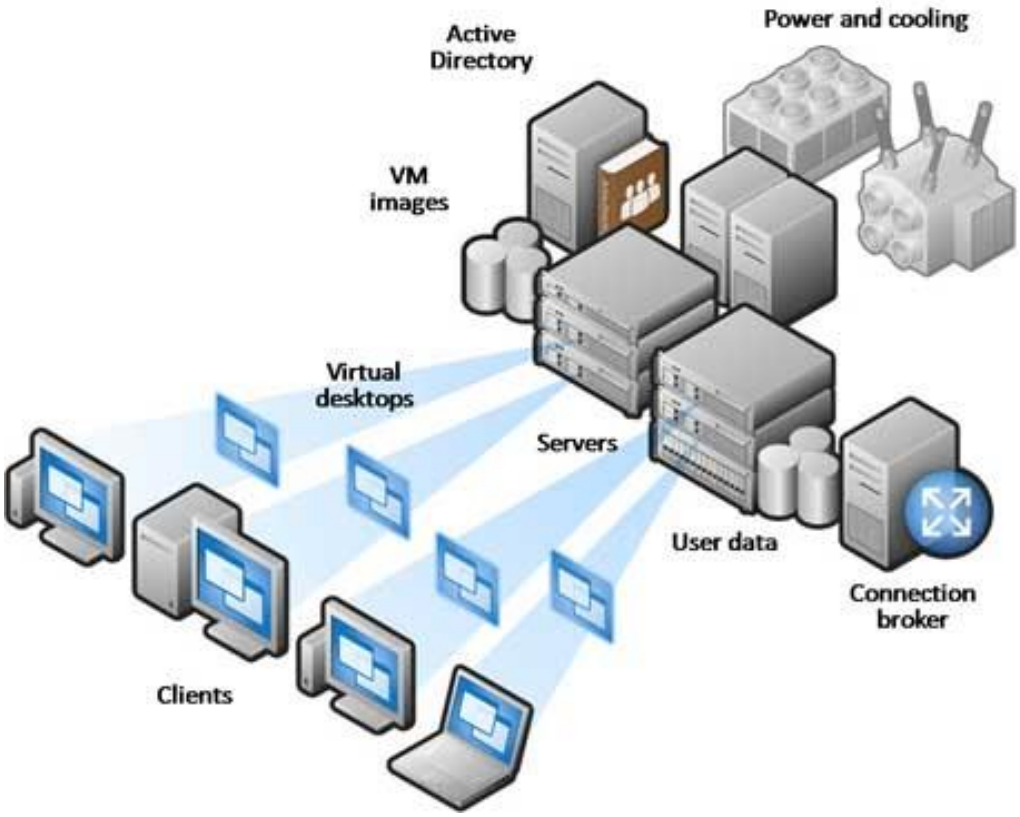
Työasemavirtualisoinnilla tarkoitetaan teknologiaa, jolla voidaan virtuaalisesti suorittaa käyttöjärjestelmää palvelimelta. Tätä tekniikkaa käyttäen vältytään fyysisiltä käyttöjärjestelmäasennuksilta, sillä palvelimelle luotu virtuaalinen työasema näyttäytyy käyttäjälle täysin samalla tavalla kuin jos käyttöjärjestelmä olisi asennettuna käyttäjän fyysiselle työasemalle. Käytännössä tämä tarkoittaa sitä, että käyttäjän työasemalle asennetussa käyttöjärjestelmässä on asennettuna virtualisointisovellus, joka tarjoaa virtualisointikerroksen verkon yli. Tämä edellyttää toimivaa verkkoyhteyttä, jonka kautta saadan yhteys palvelimeen tai pilveen.

Virtuaalityöasemissa voidaan käyttää räätälöityjä sovelluksia, asetuksia ja resursseja käyttäjän toiveiden tai tarpeiden mukaisesti. Virtualisoinnin kautta pystytään lisäksi tallentamaan data turvallisempaan ympäristöön palvelimelle tai pilveen, kuin fyysisesti käyttäjän koneelle, joka saattaa vaikkapa kadota tai mennä rikki. Data on myös näin helpommin saatavilla myös muilla laitteilla sekä muille sallituille käyttäjille.

Tiedostoille ja kansioille voidaan luoda luku- ja kirjoitusoikeudet käyttäjien mukaan. Työasemavirtualisointi myös mahdollistaa useamman virtuaalisen järjestelmän ajon, jolloin voidaan samanaikaisesti käyttää useita eri käyttöjärjestelmiä. Päätelaitteena voi tavallisen työaseman lisäksi toimia vaikkapa tablet-laite, kannettava tietokone, thin client tai älypuhelin.

Työasemavirtualisoinnissa käyttäjän data sijaitsee palvelimella tai pilvessä, josta se on käytettävissä laitteesta tai paikasta riippumatta, kunhan palvelimeen tai pilveen saadaan verkkoyhteys. Koska virtualisoinnissa yhteiset resurssit jaetaan kaikkien käyttäjien kesken, näyttäytyy yhdelle käyttäjälle varattu tallennustila yhtenä loogisena alueena. Virtualisoinnissa data ja työt voidaan varmistaa tekemällä virtuaalisesta työasemasta klooni palvelimelle. Näin myös vikasietoisuus paranee.

Työasemavirtualisoinnin kautta saavutetut taloudelliset hyödyt ovat aina riippuvaisia kohteesta, mutta esimerkiksi Kankaanpään kaupunki on säästänyt työpytävirtualisoinnin kautta useita satoja tuhansia euroja. Käytännössä työasemien elinikä pitenee, ylläpidon kuormitus helpottuu ja työnteko tehostuu paranevan suorituskyvyn myötä. Kankaanpään kaupungilla on noin tuhat työasemaa käytössä, joista 60-70 on virtualisoituja. Kaupungilla on tarkoituksena lisätä virtualisoinnin määrää, joten jatkossa säästöjä syntyy entisestään. (Kolehmainen, 2011.)



KUVA 2. Työasemavirtualisointi. (Pronier, 2012)

3 VIRTUALISOINTI MOBIILIALUSTOILLA

Virtualisointi mobiilialustoilla toimii hyvin pitkälti samalla tavalla kuin perinteisellä työasemalla. Teknologian nopean kehityksen vuoksi voidaankin nykyiset kannettavat laitteet luokitella tietokoneiksi nekin. Mobiililaitteissa käytetään samaan tapaan eri komponentteja kuin tietokoneissakin, kannettavuus huomioon ottaen tietysti. Näistä komponenteista yhdessä syntyy laite, joka prosessoi dataa.

Mobiililaitteiden avulla saatava hyöty ja rooli yrityksille on jo niin suuri, että myös virtualisointia on alettu tuomaan niille vauhdilla esiin. Mobiilivirtualisoinnilla työntekijän on mahdollista käyttää omaa laitteistoaan työpaikan verkossa esim. BYOD-mallin mukaisesti. BYOD, eli Bring Your Own Device, mallissa työntekijä voi tuoda oman laitteensa työpaikalle ja käyttää samalla laitteellaan omia ohjelmiaan, sekä yrityksen sisäisiä järjestelmiä. Erilaisia toteutustapoja on kuitenkin muitakin.

Tämä tuo mukanaan riskin haavoittuvuuksista, sillä omien ja yrityksen sisäisten järjestelmien käyttö rinnakkain saattaa altistaa yrityksen tietoturvan uhatuksi. Myös käyttäjät itse saattavat toimia omilla laitteillaan harkitsemattomasti, ja siirtää yrityksen arkaluontoista materiaalia ja tiedostoja omalle tallennusmedialleen, josta tieto saattaa joutua vääriin käsiin. Kannettavien laitteiden ollessa kyseessä, on myös mahdollista, että laitteen omistaja hukkaa sen tai se tulee varastetuksi.

Yhdenmukaisuuksistaan huolimatta, pitää mobiilialustojen virtualisoinnissa ottaa huomioon myös laitteiston suorituserot. Älypuhelimissa, tableteissa ja muissa kannettavissa laitteissa on moderneihin työasemiin verrattuna usein vähemmän muistia, hitaammat suorittimet ja vaatimattomammat näytönohjaimet. Tämän vuoksi virtualisointiympäristön tuleekin olla sujuva käyttää. Virtualisoinnin etuna toki on, että päätelaitteelta ei vaadita juuri siksi niin paljoa tehoa, koska varsinainen sovellus suoritetaan palvelimella. Virtualisointiympäristön valinta myös vaikuttaa siihen, mitä laitteita ja käyttöjärjestelmiä kyseinen ympäristö tukee. Optimaalisin valinta luonnollisesti olisikin se, joka tukee mahdollisimman useaa mobiililaitetta ja käyttöjärjestelmää. Virtualisointialustan valinta onkin yritykselle suhteellisen hankalaa, koska yrityksen tulisi ottaa huomioon tulevaisuuden haasteet ja muutokset.

IT-ala on jatkuvassa muutoksessa ja tulevaisuutta on hankalaa ennustaa. Esimerkiksi tablet-laitteiden näin vahvaan esiintuloon ei monet vielä vuosia sitten uskoneet, mutta nyt niiden käyttäminen on siirtynyt vapaa-ajan käytöstä myös työkäyttöön. Lisäksi suurissa yrityksissä työntekijöiden käyttämien kannettavien laitteiden kirjo saattaa olla todella suuri, eikä tulevista trendeistä voida vielä tietää.

3.1 Mobiililaitteet

Mobiililaitteiksi nykyään mielletään laitteet jotka ovat keveitä, pieniä ja helppoja kuljettaa mukanaan. Pienestä koostaan huolimatta näihin laitteisiin pakkautuu koostaan huolimatta melkoinen suoritusteho. Kännykät, kannettavat tietokoneet ja tabletit eroavat kuitenkin toisistaan niin rautapuolensa kuin käyttöjärjestelmiensäkin suhteen. Tämän vuoksi virtualisointisovelluksen valinnassa tulisikin ottaa huomioon tuetut käyttöjärjestelmät, jotta työntekijät saavat laitteensa toimimaan virtuaaliympäristössä.

Laitteiden laaja valikoima aiheuttaa IT-tuelle ja ylläpidolle usein vaikeuksia. On hankalaa hallita jokaista laitetta erikseen ja antaa käyttäjälle henkilökohtaista käyttötukea. Avainasemassa onkin yrityksen toimiva BYOD-strategia, sekä työntekijöiden koulutus. Yrityksen on myös mahdollista harjoittaa CYOD-mallia, jossa yritys itse tarjoaa työntekijöilleen mahdollisuuden valita käytettävän laitteensa listalta, jonka yritys on päättänyt. Täten yritys saa vähennettyä käytettyjen laitteiden kirjoa, mutta joutuu itse kustantamaan laitteet työntekijöilleen.

3.1.1 Android

Android on Googlen tuottama avoimeen lähdekoodiin perustuva mobiililaitteiden käyttöjärjestelmä. Sitä käyttää monet älypuhelinvalmistajat, kuten esimerkiksi HTC, LG, Samsung ja Sony. Lisäksi monissa tablet-laitteissa käytetään Androidia. Koska se perustuu avoimeen lähdekoodiin, on myös sovellusten kehittäminen sille ilmaista. Androidille löytyykin kattava valikoima erilaisia maksuttomia sekä maksullisia

sovelluksia. Avoimuus myös mahdollistaa itse käyttöjärjestelmän muokattavuuden. Avoimuuden myötä vaarana on kuitenkin mahdolliset haittaohjelmat ja BYOD-käytössä Android laitteistossa tuleekin varmistua riittävästä tietoturvasta ja erottaa henkilökohtaiset sovellukset yrityksen omista. Yrityskäytössä Android koetaan haastavaksi juuri avoimuudestaan johtuen. Googlen myötä laitteissa on vahva kytkös Google-tiliin, jolloin käyttäjällä on mahdollisuus käyttää googlen kalenteria, gmailia, sosiaalista mediaa ja muita ohjelmia. Androidin viimeisin päivitys on 4.4 (Kit Kat). (Androidsuomi.fi, 2013)

3.1.2 iOS

iOS on Applen kannettavien laitteiden käyttöjärjestelmä. Sitä käytetään iPhoneissa, iPadeissa ja iPod Touch-multimedialaitteissa. Koska iOS on suljettu arkkitehtuuri, on sen muokattavuus perin hankalaa. Toisaalta, tämä helpottaa yrityskäytössä laitteen hallintaa ja lisää tietoturvaa. Apple iOS mullisti aikanaan kosketusnäyttöjen käytön helpolla, mutta sujuvalla käytettävyydellään. Viimeisin käyttöjärjestelmäpäivitys tunnetaan nimellä iOS 7. iOS:n suljetun arkkitehtuurin vuoksi sitä voidaan pitää sovellustensa puolesta turvallisempana, kuin esimerkiksi Androidia, sillä sovellukset asennetaan Applen omasta kaupasta. Ongelmia tässä taas synnyttää käyttäjien halu päästä muokkaamaan käyttöjärjestelmää ja sovelluksia, jolloin he saattavat ns. jailbreakata eli mahdollistaa kolmansien osapuolien sovellusten suorittamisen laitteella. Jailbreakattu laite on huomattavasti alttiimpi viruksille ja siksi tällaisen laitteen pääsy yrityksen verkkoon onkin riski.

3.1.3 Windows Phone

Microsoftin kehittämä Windows Phone on mobiilikäyttöjärjestelmä, jota käyttävat muun muassa Nokia, HTC ja Samsung. Sen viimeisin versio on Windows Phone 8.1. Microsoftin ja windowsin myötä laitteistolla on vahva integraatio muihin microsoftin tuotteisiin ja tileihin. Yrityskäytössä tämä luonnollisesti helpottaa työntekoa, koska toimistoissa ja yrityksissä valtaosin on jo windows-ympäristö käytössä itse

työasemilla. Näinollen tiedostojen luominen, muokkaaminen ja avaaminen käy helposti myös mobiililaitteella.

Windows Phonen lähestymistapa tietoturvaan on mielenkiintoinen: laitteissa ei ole vakiona lainkaan virustorjuntaohjelmistoa. Syy tälle on siinä, että laitteet on pyritty valmistamaan niin, että suoritettavat ohjelmat ovat joko HTML5 tai .NET- pohjaisia, ja Windows Marketplace sovelluskaupasta asennettavissa, jolloin voidaan varmistua siitä että kyseinen sovellus on turvallinen. Täten jokainen Windows Marketplacesta ladattava sovellus onkin Microsoftin sertifioima. (Paananen, 2012)

3.2 Bring Your Own Device eli BYOD

Nykyajan IT-keskeisessä työmaailmassa työntekijöiden tulee olla lähes aina tavoitettavissa. Kännykät ja kannettavat tietokoneet ovat olleet jo pitkän aikaa työelämässä arkipäivää, ja nyt myös muut mobiililaitteet lisääntyvät koko ajan. Ongelmana on kuitenkin ollut se, että yritys haluaa tietoturvan ja laitteiden hallittavuuden vuoksi järjestää työntekijöilleen erikseen työpuhelimet sekä muut laitteet, kun taas työntekijät itse haluaisivat mieluusti käyttää omia, tuttuja laitteitaan. Ratkaisuksi tähän tulee virtualisointialusta, jolla luodaan laitteeseen kaksi erillistä tilaa; henkilökohtainen- sekä työprofiili, jotka ovat käytettävissä samanaikaisesti.

BYOD:n keskeisenä ajatuksena on nimensä mukaisesti oman laitteen käyttö työpaikalla. Koska teknologian kehittymisen myötä suuri osa työvoimasta omistaa älypuhelimia, tabletteja ja muita kannettavia laitteita, koetaan oma laite tutuksi ja sitä haluttaisiin käyttää hyödyksi myös työpaikalla. Aiemmin omien laitteiden käyttö työpaikalla on aiheuttanut ongelmatilanteita IT-hallinnolle, mutta juuri tähän BYOD tarjoaa korjauksen. Näin myös pystytään karsimaan työssä vaadittavien laitteiden lukumäärää.

VMwaren Euroopassa tekemän tutkimuksen mukaan työntekijät haluavat yhä useammin käyttää työssään mobiililaitteita ja -sovelluksia. Yli puolet pohjoismaisista toimistotyöntekijöistä kokee, ettei heidän työpaikka ole tarjonnut heille tarpeeksi tehokkaita työn vaatimia mobiileja työvälineitä. Tasan puolet vastaajista harkitsisi

jopa työpaikan vaihtoa, jos he eivät voisi käyttää mobiililaitteita työssään. (Talouselämä, 2013.)

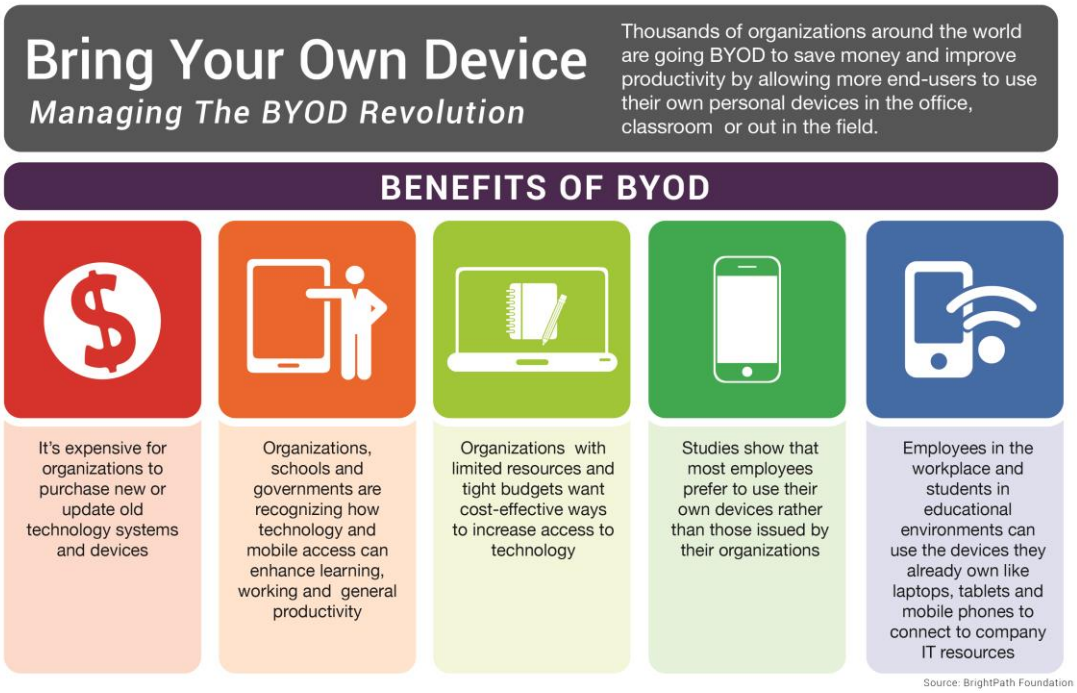
BYOD:n lisäksi yritysmaailmassa nouseva trendi on CYOD. Termi on lyhenne sanoista Choose Your Own Device, eli valitse oma käytettävä laitteesi. Tässä mallissa yrityksellä on lista hyväksytyistä laitteista, jolta työntekijä voi valita tarpeisiinsa sopivimman ja mieleisimmän. Näin yritys pystyy rajaamaan käytettyjä laitteita omien intressiensä mukaan ja tietoturvariskit pienenee ja hallittavuus lisääntyy. Haittapuolena yritykselle toki on, että tämä malli on kalliimpi kuin BYOD.

KUVA 3. BYOD:n tavoite (Comm Solutions, 2012)

3.2.1 Edut

Suuri osa työntekijöistä kokee miellyttäväksi käyttää työpaikallaan omaa, tutuksi tullutta laitettaan. BYOD-mallin myötä tämä onkin yrityksessä mahdollista ja

käyttäjä pystyy työskentelemään omalla laitteellaan. Yhtenä tämän käytännön etuna on se, että käyttäjä tuntee oman laitteensa jo valmiiksi ja pystyy näinollen usein ratkaisemaan lähitukea vaativia ongelmia itse. Oma mobiililaite on myös luontevaa kantaa mukanaan kokouksiin, seminaareihin ja tapaamisiin. Käyttäjät myös usein pitävät omasta laitteestaan parempaa huolta kuin yrityksen laitteistosta. Käytännön myötä yritys säästää myös laitehankintakuluissa, kun varsinkin nuoremmat työntekijät haluavat käyttää omia laitteitaan. Usein myös työmoraali on korkeampi omalla laitteella työskennellessä. (Maxwell, Kerry, 2013.)



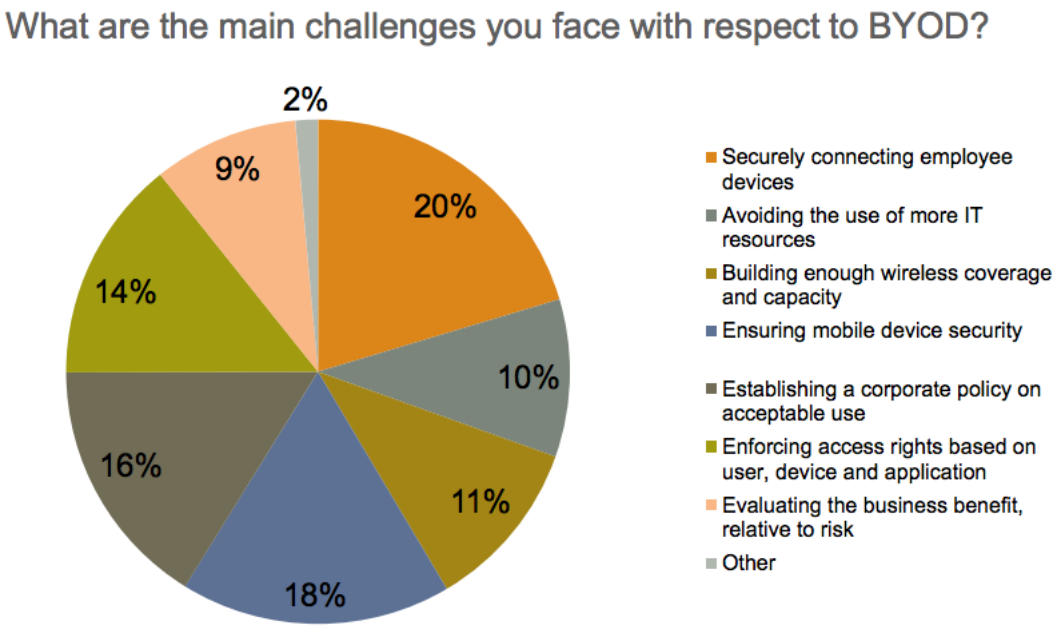
KUVA 4. BYOD:n hyötynäkökulmia. (Business Guardian, 2012)

3.2.2 Haitat

Omien laitteiden käyttö tuo mukanaan myös haittapuolia. Eri laitteistopohjan ja merkkien käyttö saattaa tuoda esiin yllättäviä ongelmia ja näihin on hankala löytää ratkaisuja. IT-tuki joutuu perehtymään moniin erityyppisiin laitteisiin, kun taas jos laitteet olisi tarjolla työpaikan puolesta. Myös virusta kantavien laitteiden pääsy yrityksen verkkoon saattaa altistaa tietoturvan uhatuksi yrityksen sisällä ja saastuttaa muita verkonkäyttäjiä ja laitteita. Myös kannettavien laitteiden kadottaminen ja arkaluontoisen datan joutuminen vääriin käsiin on suuri uhka. Huolestuttava piirre on myös se, että Check Pointin tutkimuksen mukaan 63% it-pomoista vastaa, ettei

yrityksellä varsinaisesti ole minkäänlaista BYOD-strategiaa henkilöstön kannettaville laitteille. (Pervilä, 2013.)

Aruba Networksin tekemän tutkimuksen mukaan omien laitteiden käyttöön liittyvistä haasteista suurimmat liittyvät laitteen ja työntekijän turvalliseen liittymiseen yrityksen verkkoon sekä laitteen omaan tietoturvaan.



KUVA 5. BYOD:n haasteet. (Aruba, 2012)

3.3 Eri valmistajien tarjoamia ratkaisuja

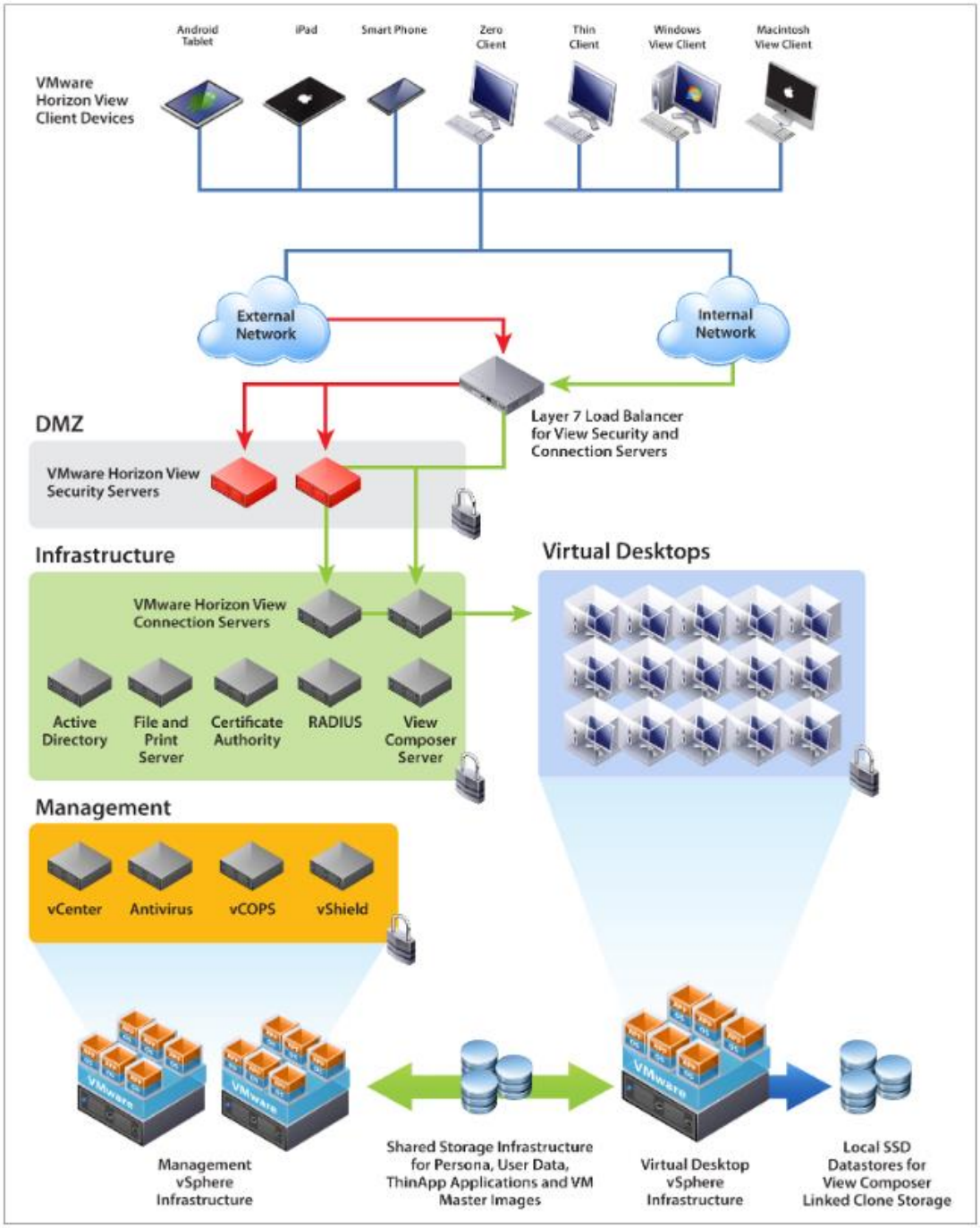
Koska myös ohjelmistotalot ovat heränneet tähän alalla kasvavaan trendiin, jossa työntekijöiden mobiililaitteille virtualisoidaan työpöytä, on erilaisia ratkaisuja ja virtualisointiympäristöjä tarjolla useita, joista käyn seuraavaksi läpi muutaman.

3.3.1 VMware Horizon View

Horizon View on VMwaren kehittämä ohjelmisto, joka tarjoaa yrityksen työntekijöille virtuaalisen työpöydän ohjelmineen. Sen tavoitteena on luoda käyttäjälle erillinen työympäristö laitteelle, erottaen sen henkilökohtaisista

applikaatioista, tiedostoista ja asetuksista. Horizon View on laitteistoriippumaton, jolloin liikkuvuus ja helppous loppukäyttäjälle korostuu. Ylläpitäjät määrittelevät työtilat loppukäyttäjille, jossa määritellään käyttöoikeudet, asetukset, resurssit sekä jaetut tiedostot. Eri käyttäjille voidaan luoda erilaisia oikeuksia, ohjelmia tai rooleja eri käyttötarkoitusten mukaan. Keskitetty hallinnointi helpottaa myös ylläpitäjien työtä. (Vmware, 2013)

Horizon View:n etuna on VMwaren historia virtualisoinnin piiristä. VMware on jo pitkään ollut yksi merkittävimmistä virtualisoinnin kehittäjistä ja palveluntarjoajista ja sille löytyy tukea varmasti. Sillä on myös luotettava maine alan piireissä.
(Vmware, 2013)



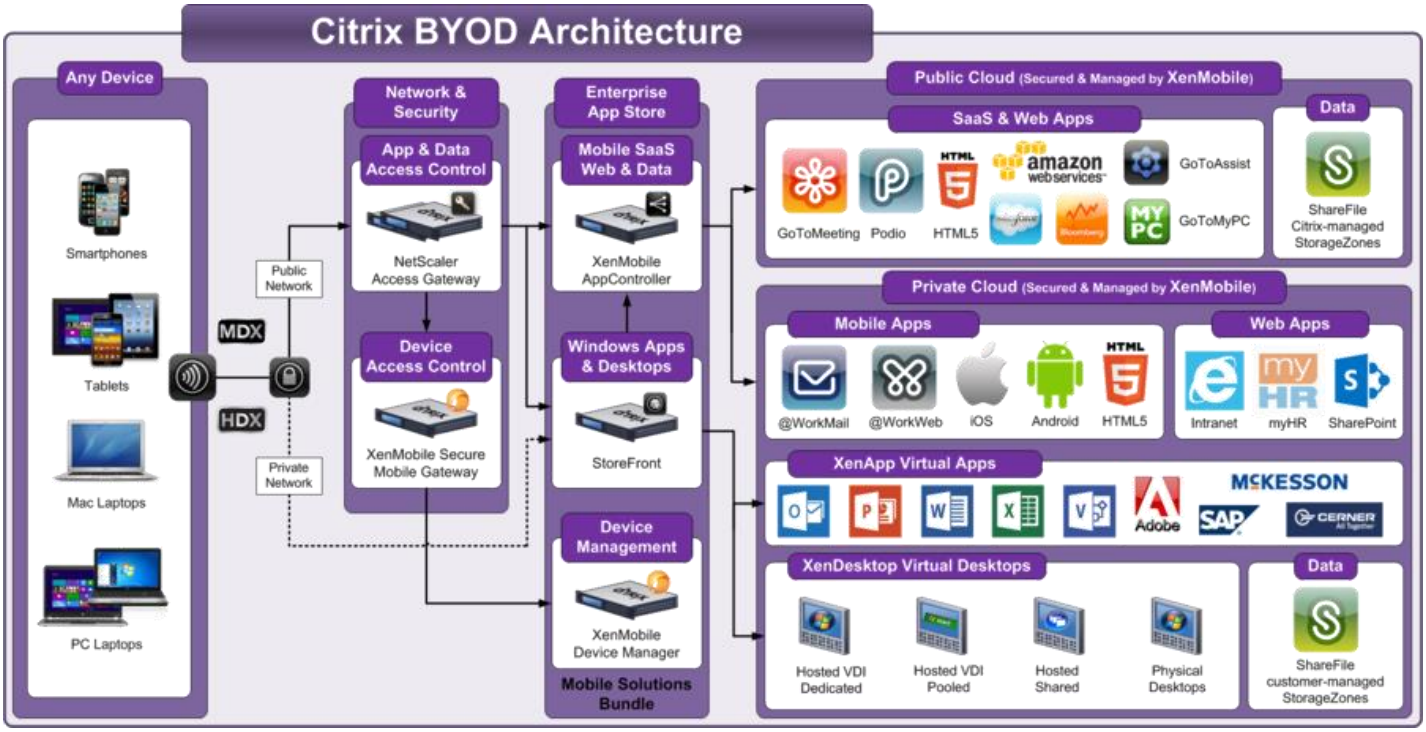
KUVA 6. VMware Horizon View:n arkkitehtuuri. (VMware, 2013)

3.3.2 Citrix XenMobile

Citrixin XenMobile on hyvin pitkälti samankaltainen tuote kuin Horizon View. XenMobilen avulla luodaan kokonaisvaltainen ratkaisu hallita mobiililaitteita, sovelluksia ja dataa, jotta käyttäjien on turvallista ja helppoa tehdä töitään omilla laitteillaan. (Citrix, 2013)

Sen keskeisenä toimijana on Worx, kokoelma mobiiliapplikaatioita, joihin kuuluvat turvattu sähköposti, web-selaus ja tiedostojenjako. Kolmannen osapuolten ohjelmien lisäys on tehty niinkin helpoksi, että se onnistuu yhden koodirivin lisäyksellä. Windows sovelluksia on mahdollista lisätä käyttäjille XenMobilen ohjelmistokaupasta, eli app storesta. (Rouse, 2013)

XenMobile on laajasti hallittavissa ja lähes jokaista yksityiskohtaa voi säätää ja asettaa käytäntöjä. Tämä on järjestelmässä toki hieno piirre, mutta saattaa tuntua joissain tapauksissa monimutkaiselta ja hankalalta.

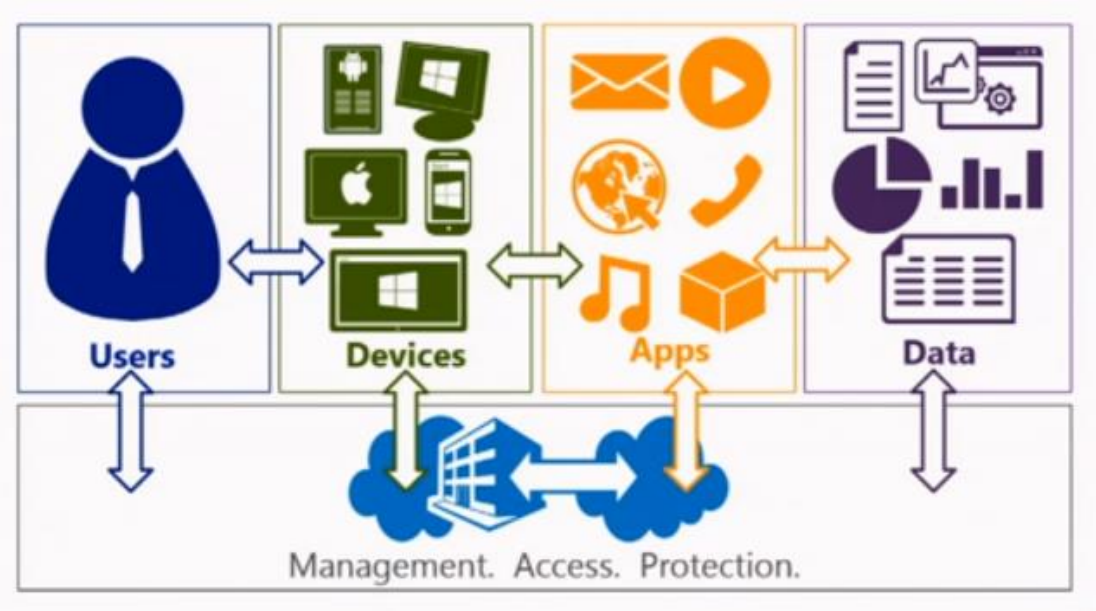


KUVA 7. XenMobile arkkitehtuuri. (Egenas R. 2013)

3.3.3 Microsoft VDI

Microsoftin Virtual Desktop Infrastructure (VDI) tarjoaa käyttäjälle virtuaalityöpöydän, jota käyttää omalla tai firman laitteistolla, firman verkossa tai ulkoisessa verkossa. Keskitetty sovellusten ja työpöytien hallinta onnistuu

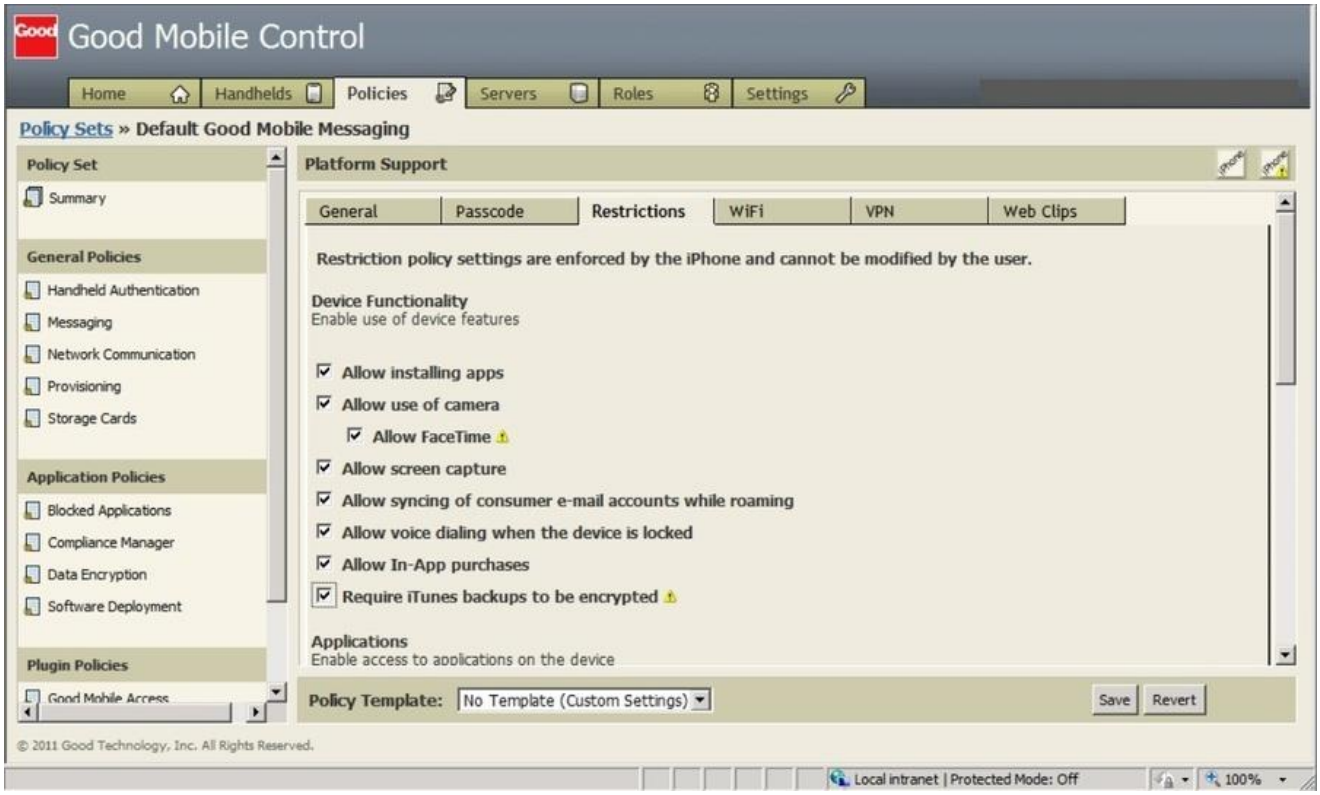
datakeskuksesta tai pilvestä ja ovat helposti suojattavissa. Käyttäjille voidaan luoda erilaisia käytäntöjä, oikeuksia ja asetuksia laitteistosta riippumatta. Tuettuja käyttöjärjestelmiä ovat mm. Windows (RT), iOS, Mac OS X ja Android. (Microsoft, 2014)



KUVA 8. Microsoft VDI arkkitehtuuri. (Wlodarz, D. 2013)

3.3.4 Good for Enterprise

Good Technology on ollut mukana kehittämässä MDM työkaluja jo vuodesta 2000, vaikka ei monelle kuluttajalle olekaan niin tuttu kuin kilpailijansa. Se tarjoaa yrityksille ja käyttäjille datakeskeisen, turvatun tavan käyttää laitteitaan työssään. Sen perimmäisenä ajatuksena on erottaa arkaluontoiset materiaalit henkilökohtaisista ohjelmista ja ympäristöstä. Sitä suositellaan erityisesti yrityksille, joille on tärkeätä salata yrityksen oma data, sähköpostiliikennne sekä erottaa kolmannen osapuolen ohjelmat yrityksen omista. Myös Good for Enterprise tukee merkittävimpiä mobiilikäyttöjärjestelmiä, eli iOS:ää, Windows Phonea sekä Androidia. (good.com, 2014)



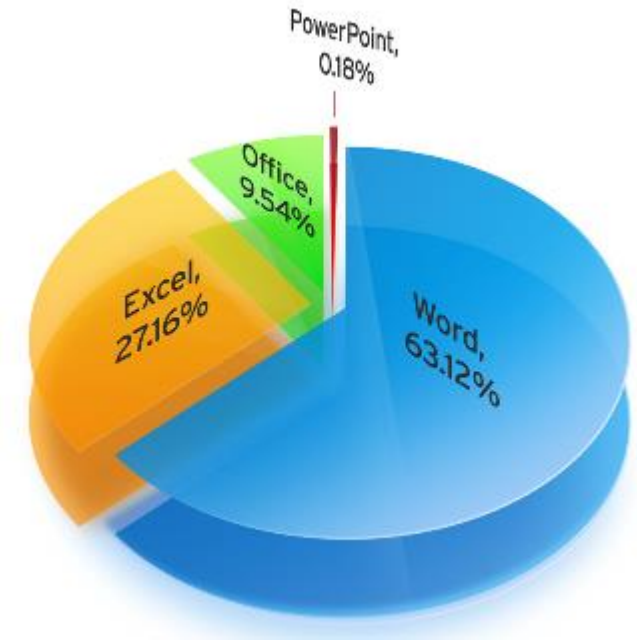
KUVA 9. Näkymä Good for Enterprise hallintaohjelmasta. (Olavsrud, T. 2013)

3.4 Tietoturva

Koska mobiilivirtualisointi tekee tuloaan niin suurella vauhdilla, jää tietoturva usein liian vähälle huomiolle. Yritykset joko soveltavat vanhoja käytäntöjään virtualisoituihin ympäristöihin tai reagoivat tilanteisiin liian myöhään. Koska yritykset haluavat säästää ylläpitokuluissa, eivätkä sijoita virtualisoinnin huomioon ottaviin tietoturvajärjestelmiin, vaan pysyttelevät perinteisissä järjestelmissään, voi pahimmassa tapauksessa syntyä vakavia aukkoja, joista dataan päästään kiinni ulkopuolelta. Vanhat tietoturvajärjestelmät saattavat myös tukkeuttaa tietoverkon kaistanleveyden, kun monistetut työasemakuvat alkavat suorittamaan päivityksiä tai järjestelmäskannauksia virusten varalta samanaikaisesti. (Trendmicro.com, 2012)

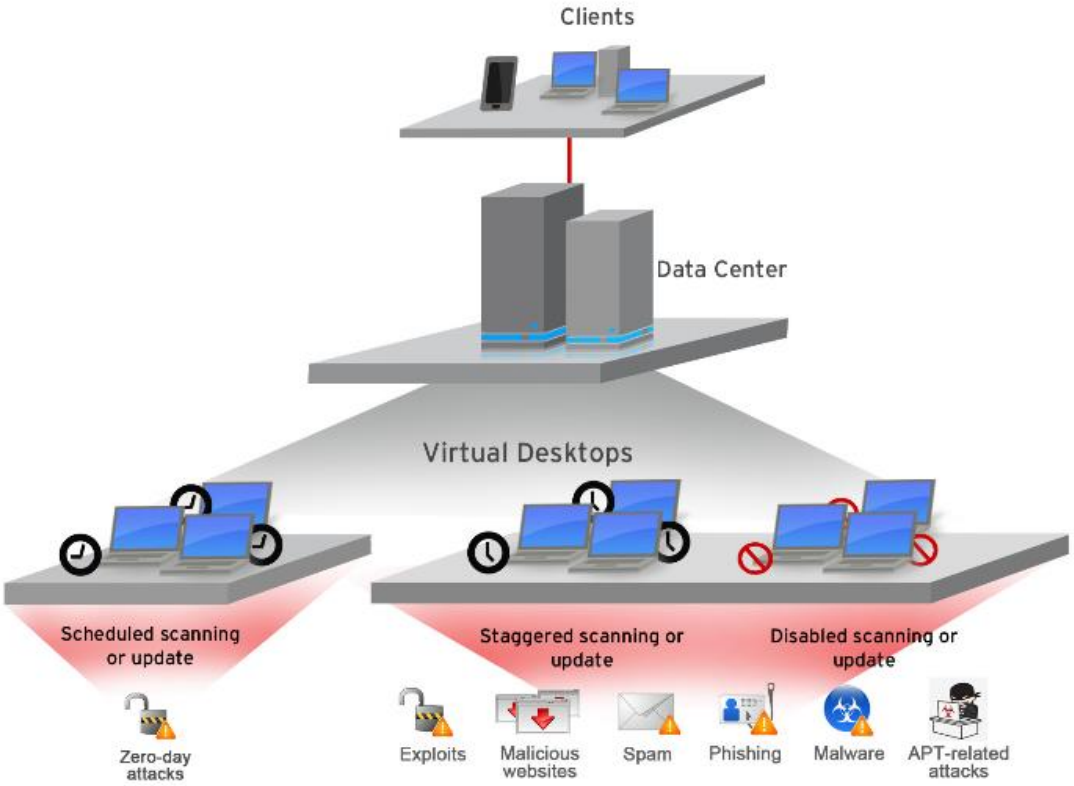
Virtuaaliset työasemat altistuvat myös fyysisten työasemien tapaan ns. zero-day haavoittuvuudelle, jossa hyökkäys kohdistuu sovelluksessa olevaa tietoturva-aukkoa kohtaan. Näitä aukkoja on löydetty mm. Microsoftin, Adoben sekä Applen

sovelluksista, jotka käyttävät automaattisia komentokäskyjä. Myös tietojenkalasteluyrityksiä saattaa tulla vastaan esim. sähköpostin liitetiedoston muodossa. (Trendmicro.com, 2012)



KUVA 10. Jakauma Microsoftin sovelluksiin kohdistuneista hyökkäyksistä (Trendmicro.com 2012)

Trend Micro on kehitellyt erityisesti virtualisoituja ympäristöjä varten oman tietoturvaohjelmiston Deep Security, joka osaa toimia optimaalisesti edellisiä uhkia kohtaan. Se on laitteistolle kevyt käyttää ja vapauttaa tilaa jokaiselta virtualisoidulta työasemalta. Näin ollen virtualisoitu työasema pystyy paremmin hyötykäyttämään resurssejaan ja vasteaika pienenee. (Trendmicro.com, 2012)



KUVA 11. Virtuaalisiin työasemiin kohdistuvat uhat (Trendmicro.com, 2012)

3.5 Thin Client

Uutena toteutus- tai lähestymistapana saattaa monelle yritykselle olla järkevää siirtyä nk. Thin Clientteihin, jotka ovat pieniä, keveitä työpöytälaitteita. Perinteisesti nämä laitteet on tunnettu nimenomaan pienuudestaan, mutta nyt esimerkiksi Dell on muuttanut Thin Clientin roolia merkittävästi uudella tuotesarjallaan, jossa otetaan virtualisointi ja pilvipalvelut vahvasti mukaan. Thin Clientiin siirtyminen saattaa olla yritykselle järkevää vaikkapa siinä tilanteessa, että yrityksen laitteisto on vanhaa ja XP-pohjaista, jolloin tämä ratkaisu on kustannustehokas ratkaisu.

Dell on tuonut markkinoille sarjan mobiileja ja pöytämallisia päätelaitteita, joissa suoritetaan pilvestä itse käyttöjärjestelmää. Päätelaitteita on perinteisestä työasemasta nk. thin clienteihin sekä Cloud Connect multimedialaitteeseen, joka

voidaan liittää vaikkapa television tai näytön MHL- tai HDMI-porttiin. Kun Cloud Connectiin liittää vielä hiiren ja näppäimistön USB- tai Bluetooth-yhteydellä, voidaan palvelu mahdollistaa monessa paikassa. Koska Cloud Connect multimedialaite on vain hieman USB-muistitikkua suurempi, on sitä myös helppo kuljettaa paikasta toiseen esim. kokouksiin, presentaatioihin tai seminaareihin.

Pilvipalvelumallin avulla data pysyy tallessa pilvessä, eikä itse laitteella ole sinänsä mitään arvoa esim. varkaalle, koska se ei sisällä itse dataa. Tämä on luonnolisesti myös yritykselle merkittävä hyötynäkökulma, kun data säilyy keskitetysti tallessa, mutta silti käyttäjien saatavilla. (Dell, 2014.)

3.6 Microsoft Direct Access

Microsoftin Direct Access on Windows Server 2008 ja sitä uudempiin Windows Server käyttöjärjestelmiin sisältyvä palvelu. Sen tavoitteena on luoda VPN-tyylinen yhteys yrityksen verkkopalveluihin. VPN-yhteydestä poiketen käyttäjän ei tarvitse luoda tai lopettaa yhteyttä itse päätelaitteelta, vaan yhteys muodostuu automaattisesti. Näin saavutetaan loppukäyttäjälle helppokäyttöinen ja suojattu yhteys yrityksen verkkoon ja etätyöskentely onnistuu helposti. Päätelaitteiden käyttöjärjestelmänä tulee olla Windows 8 Enterprise, Windows 7 Ultimate tai Windows 7 Enterprise, joille Direct Access tuki löytyy. Tästä syystä Direct Access rajaakin joitain mahdollisuuksia, mutta yrityksissä, joissa on vahva Windows laitepohja, on tämän tekniikan käyttö varmasti harkinnan arvoista. (Microsoft, 2014)

4 VERTAILU

Käytettävän virtualisointialustan valinta riippuu pitkälti organisaation rakenteesta ja sen tarpeista. Yrityksen tulee tehdä omat johtopäätöksensä siitä, mitä ominaisuuksia se oikeasti tarvitsee. XenMobilen ja Horizon View:n puolesta puhuu laaja muokattavuus, mutta jonkuille yrityksille näin suuri hiominen ja pikkutarkkuus tuskin on tarpeen ja tällöin käyttöön voisi sopia paremmin Good for Enterprise. Microsoftin VDI:n etuna tai haittana voidaan nähdä vahva integraatio Microsoftin tuoteperheeseen.

Erilaisesta lähtökohdista lähtevät Dellin Thin Client- laitteet sekä Microsoftin Direct Access ovat nekin varmasti joillekin erinomainen valinta. Dellin pilvipohjaiset laitteet kannattaa ottaa harkintaan, jos yrityksen laitteistokanta on vanhaa ja sitä ollaan päivittämässä uuteen. Direct Access taas on palvelu, jonka näkisin sopivan yrityksiin, joissa työskennellään lähes yksinomaan Microsoft ja Windows-ympäristössä.

Tutkiessani eri toteutusympäristöjä, kävi selväksi se, että jokainen niistä tukee ainakin yleisimpiä mobiilikäyttöjärjestelmiä. Jokaisen tuotteen perusperiaate myös on sama: mahdollistaa työnteko missä ja milloin tahansa, kunhan verkkoyhteys on saatavilla. Jokaisen iskulauseena myös on uuden teknologian kautta saavutetut taloudelliset säästöt, mutta tätä voidaan pitää hieman kyseenalaisena, sillä asia riippuu hyvin pitkälti yrityksestä. Pienet yritykset saattavatkin pärjätä aivan mainiosti ilman virtualisointia tai BYOD-mallia, mutta suuremmille yrityksille tämän teknologian käyttöönotto saattaa oikeasti säästää rahaa ja aikaa.

Jokainen käsiteltävistä toteutusympäristöistä mainostaa omaa tuotettaan monipuolisena järjestelmänä, joka ratkaisee yrityksen koko mobiilivirtualisoinnin ja vähän vielä päälle. Näihin mainospuheisiin tulee kuitenkin suhtautua tietyllä kritiikillä, sillä tietysti ohjelmistotalot mainostavat juuri omaa tuotettaan parhaana. Paras tapa olisikin päästä kokeilemaan itse tuotetta, joka ei minulle henkilökohtaisesti ollut valitettavasti mahdollista.

5 POHDINTA

Mobiililaitteiden työpöytävirtualisointiin, kuten myös virtualisointiin yleisesti, on suurenevan kysyntänsä vuoksi paljon halukkaita palveluntarjoajia ja eri ratkaisuja. On yrityksen vastuulla tehdä päätös siitä, mikä monista mahdollisista ehdokkaista valitaan yrityksen käyttöön. Yrityksen tulee punnita tarkkaan saavutetut hyödyt sekä mahdollisesti eteen tulevat ongelmat ja riskit. Työtapojen ja aikojen muuttuessa asiaan on kuitenkin reagoitava ja tehtävä tarpeelliset toimintastrategiat. Oman laitteen käyttö työpaikalla on nykyaikaa ja ilman sitä menetetään monia kilpailuetuja kilpailjoihin nähden ja pidetään omat työntekijät tyytyväisinä.

Haasteina BYOD-käytännössä ovat tietoturvauhat. Laitteiden omat sovellukset pitää pystyä erottamaan yrityksen sisäisistä ja tehdä käyttäjille selväksi miten käyttää järkevästi laitettaan. Yrityksen tietoja käsitellessä tulisi käyttää vain yrityksen omaa virtualisointiympäristöä, eikä jakaa tai tallentaa tiedostoja esim. dropboxiin tai muutenkaan käyttää tällöin kolmansien osapuolien ohjelmia.

Myös laitteiden katoaminen tai varastaminen saattaa koitua yritykselle kalliiksi. Pienet laitteet hukkuvat helposti ja näin yrityksen data on tuuliajolla ja saattaa aiheuttaa yritykselle merkittävät vahingot. Tähän onkin virtualisointisovelluksissa reagoitu siten, että yrityksen data pystytään joko pyyhkimään laitteesta pois tai estämään siihen pääsy. Laitteissa on myös itsessään jo usein jäljitysohjelma, jolla kadonnut laite voidaan paikantaa. Paras ratkaisu tähän olisikin säilyttää yrityksen data omalla palvelimella ja estää ulkopuolisten pääsy siihen.

Mobiililaitteiden käytössä tulee myös ottaa huomioon laitteiden erot ja monimuotoisuus verrattuna varsinaisiin työasemiin. Joidenkin laitteiden käyttö ei ole yhtä sujuvaa kuin fyysisellä näppäimistöllä ja hiirellä varustetut työasemat. Tämän vuoksi virtualisointisovelluksessa tulisikin ottaa huomioon kosketusnäytöt ja muut erilaisille mobiililaitteille ominaiset käyttötavat. Mielenkiintoisia uusia innovaatioita ovat esim. Dellin pilvipalveluihin perustuvat päätelaitteet, jotka muokkaavat käsitystä itse työasemasta. Onkin mielenkiintoista seurata, miten laajalti vaikkapa Clou Connect- multimedialaite leviää ja onko siitä tulevaisuuden trendilaitteeksi.

Mobiilivirtualisoinnin alati kasvavan trendin myötä yrityksille myös myydään teknologiaa, jota ne eivät välttämättä tarvitse. Esimerkiksi pieni yritys saattaa pärjätä vallan mainiosti ilman kyseistä teknologiaa, mutta kokevat jäävänsä liiketoiminnassa jälkeen, jos he eivät siirry ajassa eteenpäin.

LÄHTEET

Androidsuomi.fi 2013
Saatavissa:
http://blog.androidsuomi.fi/mika-on-android/

Citrix 2013
Saatavissa:
http://www.citrix.com/products/xenmobile/overview.html

Conroy, S. 2010. History of Virtualization.
Verkkojulkaisu.
Saatavissa:
http://www.everythingvm.com/content/history-virtualization

Dell 2014

Saatavissa:

http://www.dell.com/fi/yritykset/p/cloud-client-computing#!tabId=C97D0185

Dittner, R. & Rule, D. 2007. The best damn virtualization book period.
Yhdysvallat:
Syngress Publishing.

Good 2013
Saatavissa:
http://media.www1.good.com/documents/WP-Data-Centric-BYOD.pdf

Kolehmainen, A. 2011 Tietoviikko
Saatavissa:
http://www.tietoviikko.fi/cio/jattisaastot+tyoasemien+virtualisoinnista+kankaanpaassa/a675998

Maxwell, Kerry 2013. Buzzword BYOD.
Verkkojulkaisu.
Saatavissa:
http://www.macmillandictionary.com/buzzword/entries/byod.html

Microsoft 2013
Saatavissa:
http://www.microsoft.com/en-us/windows/enterprise/products-and-technologies/virtualization/operating-system/default.aspx

Paananen, V. 2012 Mr. Windows Phone Finland- blogi
Saatavissa:
https://mrwpf.wordpress.com/2012/04/27/windows-phone-haitaohjelmat-virustorjunta-ja-palomuuri/

Pervilä, M. 2013 Tietoviikko
Saatavissa:
http://www.tietoviikko.fi/cio/tama+ittrendi+aiheuttaa+jattiriskit/a908041

Rouse, M searchconsumerization.techtarget.com
Saatavissa:
http://searchconsumerization.techtarget.com/definition/Citrix-XenMobile

Talouselämä 2013
Saatavissa:
http://www.talouselama.fi/uutiset/tata+ei+kannata+tyopaikalla+kieltaa++tutkimus+kielto+johtaisi+joukkopakoon/a2189423

Trend Micro 2012
Saatavissa:
http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/rpt_extending_traditional_security_to_vdi.pdf

VMware 2013
http://www.vmware.com/products/horizon-view/

Wikimedia Foundation, Inc. 2010. Virtualization
Saatavissa:
http://en.wikipedia.org/wiki/Virtualization

Wikimedia Foundation, Inc.
2010. Timeline of virtualization development
Saatavissa:
http://en.wikipedia.org/wiki/Timeline_of_virtualization_development

Kuva 1. Wikimedia 2010. Hardware virtualization
Saatavissa:
http://commons.wikimedia.org/wiki/File:Hardware_Virtualization.jpg

Kuva 2. Pronier J-Y. 2012. Figure enterprise-vdi
Saatavissa:
http://jypronier.wordpress.com/2012/05/07/le-vdi-une-approche-salvatrice-pour-le-byod/

Kuva 3. Comm Solutions. 2012 BYOD:n tavoite

Saatavissa:

http://www.commsolutions.com/press-releases-news/comm-solutions-company-completes-aruba-networks-clearpass-specialization/

Kuva 4. Business Guardian. 2012. Benefits of BYOD
Saatavissa:
http://guardian.co.tt/business-guardian/2012-12-06/why-businesses-are-embracing-bring-your-own-device

Kuva 5. Aruba. 2012. Aruba networks study byod
Saatavissa:
http://www.zdnet.com/blog/btl/byod-inches-along-in-europe-middle-east-africa/77605

Kuva 6. VMware. 2013. Horizon View architecture
Saatavissa:
http://www.vmware.com/files/pdf/view/VMware-View-Evaluators-Guide.pdf

Kuva 7. Egenas, R. 2013. Citrix BYOD architecture
Saatavissa:
http://richardegenas.com/2013/02/28/citrix-byod-architecture-overview-xenmobile-mobility/

Kuva 8. Wlodarz, D. 2013 Microsoft VDI architecture
Saatavissa:
http://betanews.com/2013/10/08/5-reasons-surface-tablets-blow-away-ipads-for-a-mobile-business-workforce/

Kuva 9. Olavsrud, T. 2013 Good for Enterprise
Saatavissa:
http://www.citeworld.com/slideshow/108879/10-mobile-device-management-leaders-help-it-control-byod-22071#slide5

Kuva 10. Jakauma Microsoftin sovelluksiin kohdistuneista hyökkäyksistä Trendmicro.com 2012
Saatavissa:
http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/rpt_extending_traditional_security_to_vdi.pdf

Kuva 11. Virtuaalisiin työasemiin kohdistuvat uhat Trendmicro.com 2012

Saatavissa:

http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/rpt_extending_traditional_security_to_vdi.pdf